

## الباب الثاني

### قضايا الكمبيوتر : الأمن - الخصوصية - الأخلاقيات

#### COMPUTER ISSUES : Security , Privacy , Ethics

بعد فترة وجيزة من تعاملك مع الكمبيوتر ستشعر بأنه كل شيء فيه محوسس ويسهل إدارته وتعريفه : الجراز بملكوناته المختلفة والبرامج بأنواعها المتباينة والشبكات التي تربط الأجهزة ببعضها البعض .. ولكنه هناك اعتبارات أخرى تؤثر تأثيرا بالغاً على مناخ عمل المنظومة الكمبيوترية ويصعب تقنينها ووضع إطار واضح لها .. هذه الاعتبارات تمثل في الواقع قضايا جديدة جدية بالبحث ، ويمكن تقسيمها إلى فئات ثلاث :

- اعتبارات الأمن
- اعتبارات الخصوصية
- الاعتبارات الأخلاقية

فإذا انتقلت بيانات تهلك في ملف قاعدة بيانات والتفت أنه هناك من تسلل إلى جهازك وعبث بهذا الملف أو دثره بالكمال ، فأعلم أنه بياناتك لم تكن في مأمن .. وإذا تبادلت رسائل سرية بالبريد



اللاكتروني مع أحد زملائك في العمل وعلمت أنه  
رئيسك قد اطلع عليها ، فستفرض هتماً  
انترالك فصوصيتك ... وماذا أعرت صديقاً لك  
برنامجاً منه تفصيلك وفوجئت بأنه طبع نخاً منه  
وباعها لحسابه الخاص ، فصدمتك تغير قضية  
أخلاقية .. والقصة - كما سنرى في هذا الباب -  
كثيرة وخطيرة وتعتبر آثاراً سلبية لعصر الكمبيوتر -  
عصر المعلومات المميكنة والاتصالات التي لا تحدها  
حدود .

## ١-٢ جرائم الكمبيوتر

### ( Computer crimes )

الكمبيوتر - على عظمة إمكانياته - مجرد آلة تطيع  
أوامرك طاعة عمياء طالما أنك تتعامل معها ببلغتها  
ونظام تشغيلها .. وكلما تعمقت في فهم دقائق  
آلة الكمبيوتر كلما زادت مرارتك في توظيفها وتوجيهها  
كيفما تريد .. والفهم المتعمق هنا سلاح ذو حدين ،  
فقد يدفع إلى المنفعة والخير - وهذا هو الهدف -  
وقد يحرمه على الإثم والشر .. الكهرباء - مثلاً -  
تخلق بيئة مثابرة : فهي تقدم للبشرية أجمل  
الخدمات ، وهي ذاتها التي تصنع إنساناً في جريمة  
قتل بشعة .

وللتعرف على طبيعة جرائم الكمبيوتر نذكر



## ٤-٢ أمن الكمبيوتر (Computer security)

رأيًا - من استعراضه جرائم الكمبيوتر - كيف أنه العمل الكمبيوتر في أمن الحاجة إلى فطنت أمنية مدروسة لمواجهة ضربات "تكنولوجية" ماهرة يتفقه عنها كل يوم العقل البشري متضامنا مع العقل الإلكتروني ،  
وتعبر "أمن الكمبيوتر" بأنه يعنى في الماضي شيئًا واحدًا محددًا : أمن الجواز نفسه خوفاً من سرقة أو إتلافه ، فكانت الاحتياطات تقتصر على إغلاق الأبواب وتثديد الحراسة .. ولله الأبواب المغلقة المحروسة لم تعد مجدية في زمنه يمد فيه السارق "يده" أميالاً وأميالاً ليصل إلى البيانات في قواعد داخل الأجهزة ، وهو بعيد تماماً عن العيون والآذان يدبر برهوى وينفذ بقاءه .

لذلك تولد لدى مديري الشركات إحساس فائق بضرورة توفير نظم وأدوات أمن على مستوى عال ، وأصبحوا يتابعونه لشراء كل ما هو حديث ومتقدم في هذا المجال .

فما هو "أمن الكمبيوتر" اليوم ؟ إنه نظام محكم لحماية أجهزة وبرامج وبيانات المنظومة الكمبيوترية للمناعة من حوادث السرقة أو الإتلاف أو التدمير أو التجسس ، وكذلك حمايتها من أخطار الكوارث الطبيعية وغير الطبيعية كالزلازل والفيضانات والحرائق والعمليات الإرهابية وغيرها .



١-٤-٢ تصريح الدخول الى منظومة الكمبيوتر  
(Allowing access to computer system)

من العناصر الأولية الرامة للنظام الأمن الكمبيوترى  
اهتمامه على وسائل التعرف على الأفراد المصرح لهم  
(Authorized persons) بالدخول الى المنظومة  
الكمبيوترية واستخدام إمكانياتها والتعامل مع برامجها  
وبياناتها ، ومنسب هؤلاء الأفراد "المفوضين" ..  
وكذلك التعرف على الأفراد غير المصرح لهم  
(Unauthorized persons) بالدخول الى المنظومة  
الكمبيوترية ومنسبهم "غير المفوضين" .  
فاذا كنت مفوضا من مكان محدد ، فكيف يمكنك  
إثبات ذلك ؟ توجد على وجه العموم أربعة  
أساليب :

- (١) الاثبات بما معه
- (٢) الاثبات بما تعرف
- (٣) الاثبات بما تفعل
- (٤) الاثبات بتحقيقه شخصيتك

(٥) الاثبات بما معه (What you have)

قد يكونه معه مفتاح أو شارة أو كارت مغناطيسى  
أو أى وسيلة أخرى من هذا القبيل تستطيع برهانه  
تدخل منه باب حجرة الكمبيوتر أو أنه تستخدم جهازا



مغلقة... فعلى ميل المثال يمكنك كارت ذو شريط  
محفظة مع الوصول الى حاسبك في أحد البنوك  
والصرف منه مع طريقه خزينة برمجة مثبتة بعيداً  
عنه البنك.

وفي الآونة الأخيرة شاع استخدام وسيلة مبتكرة  
تسمى "الشارة النشطة" (Active badge)  
وهي عبارة عن كارت مزود بدوائر إلكترونية دقيقة  
يضعها الشخص على صدره طوال فترة تواجده بالعمل،  
فيسل الكارت أشعة تحت حمراء (Infrared)  
ليستقبلها عدد كبير من الأجهزة الصغيرة الحاملة  
(Sensors) المركبة في أنحاء متفرقة من المبنى..  
وبواسطة هذا النظام يتخذ تحديد المكان الذي  
يذهب إليه الشخص في أي لحظة، ويسهل بذلك  
ضبط غير المفوضين الذين يحاولون الدخول الى  
مواقع عمل الكمبيوتر.

وتشير الشارات النشطة جداً وامتعا، إذ  
يعتبرها الكثيرون قيداً على حريتهم ودليلاً على  
عدم ثقة الإدارة في أمانتهم.

### (٢) الاثبات بما تعرف (What you know)

الوسائل المعتادة لأسلوب الاثبات بما تعرف  
هي كلمات السر (Passwords) وأرقام  
التحيز (Identification numbers) .. ولاشك



أنك شاهدت - مثلا - الأقفال السرية  
(Cipher locks) التي لا تفتح إلا بمجموعة  
أرقام معينة .. لاحظ أيضا أنك لا تستطيع  
استخدام خزانة البنك المبرمجة إلا بواسطة  
رقم مميز يوصلك (بالإضافة إلى الكارت ذى  
الشريط المغنط الذى أشرنا إليه سابقا) .

### (٣) الأدلة بما تفعل (What you do)

يعتمد هذا الأسلوب على توقيع الشخص  
(Person's signature) .. ورغم أنه تقليد  
التوقيعات ليس مبررا إلا أنه التزوير دائما  
وارد .. وفى الحقيقة إذا كان نظام التوقيعات قد  
أثبت نجاحا فى العلاقات البشرية ، فإنه ينبغي  
ألا يعول عليه كثيرا فى التعاملات الآلية .

### (٤) الأدلة بتحقيق شخصيتك

### (Who you are)

يستحوذ هذا الأسلوب حاليا على اهتمام كبير من  
المشتغلين بأسم الكمبيوتر ، ففيه تطبق نظريات  
علم "القياسات الحيوية" (Biometrics) الذى  
يختص بعمليات قياس الموصفات الجسدية للإنسان .  
وأشهر وسيلة هنا هى بصمات الأصابع



(Finger-prints) ، وقد تبدو للوهلة الأولى وسيلة قديمة وغير مناسبة .. ولكننا تخلصت الآن من "الجبر والخنامة" ، وأصبح كل المطلوب من الشخص مجرد وضع إصبعه لشوانه معدودة في ماكينة صغيرة لتحقيق الشخصية .

والوسيلة الثانية تعتمد على تمييز الصوت<sup>(١)</sup> (Voice recognition) .. فكل إنسان نبرات وفصائل صوتية خاصة به - دونه غيره - ويمكن رصدها بأجهزة دقيقة .

والوسيلة الثالثة - الحديثة و الشيقة - تقوم على تمييز شبكية العين (Retina) .. فقد ثبت أنه شبكية عين كل إنسان تحتوي على ملايين الخلايا الحاسة للضوء مرتبة في نمط معين لا يتكرر مع أي إنسان آخر .. فإذا نظر الشخص بعينه داخل جهاز صغير مصمم لهذا الغرض ، أمكنه التحقق من شخصيته على أساس نمط شبكية عينه .

## ٢-٤-٢ خطة مواجهة الكوارث (Disaster recovery plan)

يجب أنه تعد المؤسسة - التي تحافظ على كيانها ومعلمها وسمعتها - خطة لمواجهة الكوارث التي قد تصير فجأة بفعل فاعل أو قضاءً وقدرًا .  
فن إيطاليا ، وعلى مدار سنة كاملة ، قامت



أو إتلافها عنه محمد ..  
ورغم أهمية إجراءات أمن الأجهزة ، إلا أنه  
فقدانه جهاز - في حد ذاته - لا يمثل مشكلة خطيرة  
للمؤسسة ، إذ أنه الخسارة المادية يسرل تعويضها  
عنه طريقه شركات التأمين ويمكنه في جميع الأحوال  
شراء جهاز جديد يحمل محل الجهاز المفقود .. ولكنه  
المشكلة الحقيقية تتمثل في الوقت الذي سيمضي قبل  
أن تتمكن المؤسسة من تدبير الأجهزة البديلة ، فأى  
جهاز يتوقف عنه العمل يؤثر بالسلب على كفاءة  
العمل ككل .. ولك أن تعلم أن مؤسسات كثيرة  
(كالبنوك ومراكز المعلومات) قد تضطر للإغلاق  
أبوابها وإمساكها بإغلاقها في غضون أيام بسبب  
خروج بعضه كيوترات من منظومة العمل .

### ٣-٤-٤ أمن البرامج (Software security)

من بدريات العمل الكمبيوترى أنه تحتفظ المؤسسة  
بنسخ بديلة (Backup copies) لجميع برامجها .. ويجب  
أن يؤخذ هذا الاحتياط مأخذ الجد دائماً حتى تنقذ النسخة  
البديلة الموقف في حالة فقدانه البرنامج الأصلي .  
ويطرح أمن البرامج قضية "ملكية البرنامج"  
(Program ownership) : فإذا صمم أحد  
المبرمجين برنامجاً لحساب شركة معينة ، فمنه يصبح المالك  
الحقيقى للبرنامج ؟ المبرمج أم الشركة ؟ ثم كيف يكونه



التصرف إذا أخذ المبرمج نخامه برامجه معه وهو ينتقل  
من شركة إلى شركة ؟ هل يمنعه أحد ؟ هل يردعه  
قانونه ؟

وللإجابة على هذه الأسئلة نقول : إذا كان مصمم  
البرنامج أحد العاملين بالشركة ، فتؤول ملكية البرنامج إلى  
الشركة ، وليس من هو المبرمج من هذه الحالة أنه يأخذ  
نسخة من البرنامج معه عند انتقاله للعمل بشركة أخرى ..  
أما إذا كان المبرمج مستشاراً فقط للشركة ، فيجب أنه ينص  
صراحة في العقد المبرم بين الطرفين على من سيصير  
مالك البرنامج - المستشار أم الشركة ؟ وإذا لم  
يذكر هذا النص في العقد ( أو إذا لم يلمس هناك عقد على  
الاطلاعه ) فإنه الطرفين - عند اختلافهما - سيدخلانه  
مقاهات قضائية وعقودية .

وتمثل عمليات نسخ برامج الكمبيوتر بدونه تصريح مشكلة  
عامة مؤرقه لم يظهر لها علاج ناجع حتى وقتنا هذا .. في  
الولايات المتحدة أصدرت المحكمة الأمريكية العليا قرار  
"حقوقي تأليف البرامج" بحيث لا يسمح بنسخ أي برنامج إلا  
بموافقة كتابية صريحة من مالك البرنامج .. وفي مصر  
بدأت شركات البرمجة تلجأ إلى القضاء بعد أن تكبدت  
خسائر جسيمة من جراء نسخ برامجها بدونه تصريح .  
ورغم ذلك فواقع الحال يقول إنه البرامج لا زالت  
تنسخ على مرأى ومسمع من الجميع مثلاً تنسخ شرائط  
الأغاني والموسيقى على أجهزة التسجيل .. والقضية  
مستمرة وساخنة ، ومنغود إليها عند مناقشتنا للاعتبارات



عصابة مسلحة بتفجير عشرة مراكز هيبوية للكمبيوتر.  
وفي نيويورك انقطع التيار الكهربائي لمدة ثلاثة  
أيام وتوقفت عمليات الكمبيوتر ومثلت مواقع  
العمل وحركات الطيران والنقل في مناطق شاسعة  
بالولايات المتحدة.

وفي كاليفورنيا هاجم إرهابيون قاعدة فاندنبرج  
(Vandenberg) الجوية، ودقروا غمة أجهزة  
كمبيوتر من النوع الكبير (Mainframe) ولاذوا  
بالفرار بعد أن تركوا وراءهم باقة من زهور البانسي  
(Pansy) وعلمة هلويايت ورسالة تقول "نتمنى لكم  
يوماً سعيداً".

ناهيك عن الزلازل والبراكين والفيضانات والأعاصير  
والجراثيم التي تلحق أضرار الخائر بالمؤسسة وقد  
تزايدت مع على سطح الأرض.

وفظة مواجهة الكوارث تتضمن كيفية التصرف عند  
مواجهة الكارثة للمؤسسة، بحيث يمكن استعادة قدرات  
عمل المنظومة الكمبيوترية للإستمرار في الجو المعتاد - أو  
سببه المعتاد - لمزاولة سائر الأنشطة .. وهناك أكثر  
من طريقة :

● فقد تختار المؤسسة أنه تعود مؤقتاً إلى الخدمة  
اليديوية والملفات الورقية التي يكون قد سبق إحصاؤها  
كبديل للملفات الالكترونية وقت الحاجة .. ولكنه العامليه  
والعمالء سيعانون من متاعب ليست هينة في فترة



توقف الخدمة الآلية .

• وقد تشتري المؤسسة وقت عمل على الكمبيوتر بمكاتب الخدمة (Service bureaus) الخاصة لمواصلة أعمالها لحيد زوال آثار الكارثة .. ولأنه كانت هذه المكاتب لا توجد في الغالب إلا بالعواصم والمدن الكبيرة .

• وأحيانا تعقد مؤسساته أو أكثر في منطقة جغرافية معينة "اتفاقية عونه متبادل" (Mutual aid pact) ، فإذا تعطل العمل في إحدى المؤسسات استعانست بإمكانات المؤسسة الأخرى بناءً على الاتفاقية .. بيد أنه فائدة مثل هذه الاتفاقيات قد تتضاءل أو تنعدم إذا ما هلت الكارثة بالمنطقة كلها وباتت المؤسسات جميعها تتخبط .

• وفي حالة الشركات والبنوك ذات الأفرع المنتشرة في مختلف أقطار العالم والتي تعتمد كلية على المنظومات الكمبيوترية العملاقة وتعتبر سلامة هذه المنظومات بالنسبة لمراسلة حياة أو موت ، فيتم تلوئيم "اتحاد" فيما بين مجموعة شركات متضامنة يسمى Consortium يتولى إقامة منظومة كمبيوترية متكاملة بديلة للجور إلى فوراً عند الخطر .. وتتكلف هذه المنظومة بالطبع مبالغ ضخمة لبنائها والحفاظ عليها واختبار كفاءتها بصورة دورية .

ومن ضمنه مراقبه تلك المنظومة نوعان من



المواقع : الموقع الساخن (Hot site) وهو مركز مجهزة تجهيزاً كاملاً بكل متطلبات العمل مع كيبوترات وبرامج وخطوط اتصال ووسائل سيطرة وأمن وغلافه ، والموقع البارد (Cold site) وهو مركز خال مريباً لأنه تنتقل إليه الشركة وتمارس كافة أعمالها ولكنه بعد تركيب الأجهزة والمعدات اللازمة. وتقوم كل مؤسسة بأعداد خططها لمواجهة الكوارث مبكراً ، كما تنبئ للعاملين فرص التدريب عليها ببيئة الحية والحيثية لكن يجيدوا تنفيذها إذا دعه ناقوس الخطر.

وتنبئ الخطة على أنه كل شيء - فيما عدا الأجهزة - يجب حفظه في مكان بديل آمن بعيد عنه مقر المؤسسة الأصلي .. فيتم حفظ البرامج وملفات البيانات الرامدة وسجلات أسماء البرامج وسجلات مواصفات الأجهزة ونسخ من نظم التشغيل وصورة من خطة مواجهة الكوارث ... الخ .. كما تغطي الخطة النقاط الأساسية التالية.

### (١) الأولويات (Priorities)

تضع الخطة قائمة أولويات للبرامج والبيانات التي ينبغي المحافظة عليها وتزليل كل العقبات للوصول إليها دائماً .. فالبنتك مثلاً ترجم ملفات أرصدة العملاء بدرجة تفوق بمراحل كثيرة جداول أجهزات العاملين.

### (٢) احتياجات الأفراد (Personnel requirements)

توضي الخطة كيفية الاتصال بالعاملين لتوعيتهم بحجم الخطر



الذي يبرهن المؤسسة وإخبارهم بالتغيرات التي ستطرأ على أعمالهم العمل ونظمه ومسائله في الظروف الجديدة الصعبة.

### (٣) احتياجات الأجهزة (Equipment requirements)

تحدد الخطة ما يحتاجه العمل من أجهزة وبرامج ومعدات وأماكن الحصول عليها وطرق تركيبها وتشغيلها من الأماكن البديلة المقترحة ... فليت كل مؤسسة عضواً في "اتحاد قوى وقادرة على اقتناء" موقع ساكن مستعد لاستضافتها في أي لحظة.

(٤) استقبال وتوزيع البيانات

### (Capture and distribution)

في هذا الجزء من الخطة تتحدد طرق إدخال البيانات إلى المنظومة الكمبيوترية البديلة واستعادة هذه البيانات (أو أجزاء منها) وتوزيعها حسب مقتضيات العمل في بيئة مختلفة وأجواء ضاغطة.

### ٣-٤-٢ أمن الأجهزة (Hardware security)

على ضوء ما سبق يمكننا القول بأنه أمن المنظومة الكمبيوترية يتضمن أمن الأجهزة وأمن البرامج وأمن البيانات .. ونبدأ بالقاء نظرة على أمن الأجهزة. أجهزة الكمبيوتر وملحقاتها - مثل كل شيء في ذلك مثل أي معدات ذات قيمة - يجب توفير الأمن والحماية لها بحيث لا تفاجأ المؤسسة بسرقة أحد الأجهزة



## الأخلاقية بعد قليل .

### ٥-٤-٢ أمن البيانات (Data security)

تجئ البيانات المملوكة اليوم على رأس قائمة  
المقتنيات الثمينة للمؤسسة ، ومن هنا يبرز الدور  
الحيو لأمن البيانات والذي يتجلى في المجالات  
الآتية :

- (١) رسم سياسة واضحة وحاسمة في شأن التعامل  
مع البيانات يكون محورها : حماية البيانات وكل  
ما يتعلق بها من معلومات من أضرار الوصول إليها  
بدونه تصدح ومن أخطار تزيفها أو تدميرها .
- (٢) استخدام كلمات السر (Passwords) وغيرها  
من طرق الحماية لقصر التعامل مع البيانات على  
الأشخاص المصرح لهم بذلك .
- (٣) تخطيط احتياجات الأمن في المراحل الأولى لتصميم  
المنظومة الكمبيوترية .. فهذا أفضل وأيسر من  
التفكير في مثل هذه الاحتياجات بعد اكتمال بناء  
المنظومة .
- (٤) دراسة القوانين والتشريعات التي تخص الأمن  
بوجه عام ، والتركيز على رصد وبلورة المشكلات  
الخاصة بأمن البيانات والمطالبة بتقنيته حلول  
لها .
- (٥) القيام بعمليات صيانة دورية لسجلات البيانات



التاريخية القيمة حتى لا تقلق بتأثير طول فترة التخزين .

وهناك خطوات يمكن اتخاذها للمساعدة في وضع سياسة أمن البيانات موضع التنفيذ ، نذكر منها :  
(أ) كلمات السر (Passwords)

ذكرنا أننا نستخدم كلمات السر لقصر التعامل مع البيانات على الأشخاص المصرح لهم بذلك .. وكلمة السر عبارة عن كلمة أو رقم أو خليط من الاثنين ، ويتم إدخالها إلى الكمبيوتر عن طريق لوحة المفاتيح . ويفضل أنه تنجز البيانات إلى فئات بحيث تحدد لكل فئة كلمة سر معينة ، وبذلك يكون التصريح المعطى للشخص يختص بفئة بيانات واحدة دون الفئات الأخرى .. كما ينبغي أنه تتغير كلمات السر مع وقت لآخر .

(ب) وسائل التحكم الداخلي (Internal controls)

يمكنه أن تكون المنظومة الكمبيوترية مزودة بملكات داخلية تعمل ذاتيا لمراقبة حركة التعامل مع البيانات ، ويتم مثلا توظيف ملف لتسجيل كل محاولات الوصول أو محاولة الوصول إلى البيانات . كما يمكنه أن يبنى نظام التشغيل (Operating system) بطرق تفرضه ضوابط فنية على محلييات الوصول إلى البيانات .. في إحدى هذه الطرق يقارن رقم المستخدم برقم البيانات فيظهر ما إذا كان الشخص



مصرحاً بالتعامل مع هذه البيانات أم أنه يتحایل للوصول إليها في الخفاء .. وفي طريقة أخرى يتم تخزين "سيرة" كل مستخدم (User profile) التي تضم معلومات كاملة عنه بما فيها فئات البيانات المصرح له بالتعامل معها ، ويرجع إلى هذه المعلومات كلما اقتضى الأمر .

#### (د) فصل الأعمال الوظيفية

##### (Separation of employee functions)

يجب أنه تفصل الوظائف المتعلقة بالعمل الكمبيوترى عنه بعضها البعض كلما أمكن ذلك .. فالمبرمج مثلاً ينبغي ألا يكون مسؤولاً في نفس الوقت عن تشغيل البرامج ، لأنه جمع شخص واحد بينه العمليه لا يعطيه فرصة كتابة برامج غير مصرح بها فحسب وإنما تمنحه أيضاً إمكانيات تجربة هذه البرامج وتغييرها والحصول منها على المعلومات التي يسعى إليها .. وفصل الوظائف وإجراء مألوف ومطبوع في الأعمال العادية ، فلا نجد مثلاً موظفاً وهيداً مسؤولاً عن أعمال تقدير المبالغ المستحقة وتحرير الشيكات اللازمة لها وتوقيع هذه الشيكات وفهمها بشعار الجمهورية ، بل يعينه أكثر من موظف للقيام بهذه الأعمال متتابعين فيكون كل واحد منهم مراجعاً لعمل زميله الذي يسبقه .

وثمة نقطة أخرى تتعلق بالتنويه : كثيراً ما تضادف موظفاً مواظباً على عمله لأقصى درجة ، لا يتأخر ولا يتغيب ولا يتأجر ولا يتذمر ولا يأخذ أي



نوع من الأجهزة .. ورغم هذه المثالية إلا أنه قد يكون متأثراً - بقصد أو بدونه قصد - بقدر كبير من المعلومات الرطبة ولا علم للإدارة بذلك .. من هنا يبحث مديرو الشركات الموظفين دائماً على القيام بأجهزةاتهم لكي يتبين ما بحوزة كل موظف من معلومات ومدى أهميتها .. وخير للإدارة أنه تكتشف هذه الخبايا والموظف في أجهزة قصيرة من أنه تكتشفها بعد انتقال الموظف للعمل بشركة أخرى.

#### (د) مراجعة الحسابات (Auditor check)

يعمل لدى معظم الشركات عدد من مراجعي الحسابات لضبط الدفاتر المالية ويدخل في نظام عملهم مراجعة كافة البرامج والبيانات .. وكأجراء آمن للملفات يكلف هؤلاء المراجعون أيضاً بمصر الأشخاص الذين تعاملوا مع ملفات البيانات في الفترات المعروفة أنه أحداً لا يهتم خلال المطالعة على أي بيان ، وكذلك البحث وسط الملفات عن أي أرقام شاذة أو سجلات غير مكتملة .. فقد يؤدي ذلك إلى اكتشاف عملية تزيف أو تدمير.

ومن ناحية أخرى توجد برامج جاهزة لمراجعة الحسابات (Audit software) يمكن بواسطتها اختبار صحة ودقة عمليات المنظومة ومخرجاتها .. وتلعب هذه البرامج دوراً في تعزيز الاحتياطات الأمنية إذ تتيح للمراجعين إمكانية أداء عملهم بدون اللجوء



الى مبرمجى الشركة .

(هـ) اختبار العاملين الجدد

### (Applicant screening)

فى نظام الأسمه الكمبيوترى ينظر الى العنصر البشرى على أنه نقطة ضعف النظام ، فالكمبيوتر لا يفعل شيئاً - مفيداً أو ضاراً - إلا بأوامر من الإنسان .. وعليه يجب تحرى الرقة المتناهية عند اختبار الأشخاص المتقدمين لوظائف شاغرة بالشركة حتى يتنى اختيار الشخص الأميه ذى السعة الطبية واستبعاد كل من يحوم حوله ملك .

### (Secured waste) تأمينه صناديقه النفايات

لا ينتبه كثير من صناديقه النفايات ، ولذلك تعتبر مصدر خطورة فى سياسة أسمه البيانات اراجع شكل (١-٢) .. فصور المستندات والطبوعات وشرائط الطبع التى تلقى بالامبالاة فى هذه الصناديق قد تحتوى على معلومات مخفورة ضرورية من الشركة أو مقصور التعامل معها على أصحاب التصاريح الخاصة .. لذلك يجب تأمين صناديقه النفايات باستدام الأنواع محكمة القفل وهرجه محتوياتها أولاً بأول تحت إشراف مسئولى الشركة .

### ٢-٥ فيروس الكمبيوتر (Computer virus)

الفيروسات - فى المصطلحات الطبية - جراثيم صغيرة



تتكاثر في الخلايا الحية وتجلب الأضرار للجسم .. وفيروس الكمبيوتر يهاجم بطريقة مماثلة الأجهزة والبرامج والبيانات ويتجهم عنه عمل كثيرة تتراوح من إرسال عبارات غريبة وإصدار أصوات مزعجة الى تدمير الملفات وإصابة الذاكرة بالشلل التام .. وتحمل كلمة فيروس معاني الخوف والتزديد والارتباك للعاملين في الحقل الكمبيوترى .. ويكفى أنه نقول إنه الفيروسات الكمبيوترية تكلف اقتصاد الولايات المتحدة أكثر من ٢ مليار دولار سنويا .  
فما هو هذا الفيروس ؟ إنه برنامج ( مجموعة من الأوامر الموجهة الى الكمبيوتر ) يكتبه صاحبه لغرضه شريف في نفسه .. وبرنامج الفيروس - كما يدل الاسم - برنامج مُقَدِّ : فهو يستقر في الذاكرة ثم ينقل عدواه الى أى برنامج يقترب منه في ذات الذاكرة .. وعندما يصاب البرنامج الجديد يصبح بدوره حاملا للفيروس ، وبرهذه الطريقة تشرى العدوى من برنامج الى برنامج .. ويتفشى الوباء ..

والفيروسات المنتشرة حاليا تفوح الحصر ، ونذكر على سبيل المثال :

### • فيروس "يانكى دودل" (Yankee Doodle)

عندما يصيب فيروس يانكى دودل ( الاسم مأخوذ من أغنية أطفال شهيرة ) إحدى المنظومات ، فإنه يجعل الكمبيوتر يصدر ضوضاء مزعجة في تمام الساعة الخامسة مساءً كل ثمانية أيام .



### • فيروس "القدس ب" (Jerusalem B)

ينشط هذا الفيروس طوال يوم الجمعة الموافق ١٣ من الشهر الميلادي .. ويأخذ في محو بيانات أى ملف يتم تحميله في الذاكرة من أقراص التخزين .

### • فيروس "الشلل" (Cascade)

يصيب هذا الفيروس نظام التشغيل (Operating system) .. ويتسبب في عدم إتمام كتابة النصوص والتعليمات ، إذ تترك بعض الحروف من الأسطر بصورة عشوائية وتتراكم في قاع شاشة العرصة .

وبالإضافة إلى الفيروسات توجد الديدان (Worms) .. ودودة الكمبيوتر هي برنامج - مثل برنامج الفيروس - ولكنه ينتقل من كمبيوتر إلى كمبيوتر عبر شبكة كمبيوترية .. وتزرع الدودة نفسها على هيئة ملف منفصل في أقراص التخزين المستهدفة .

ومن أشهر البرامج الدودية ذلك البرنامج الذي فطمه طالب يدعى "روبرت موريس" (Robert Morris) بجامعة "كورنيل" (Cornell) الأمريكية وتملكه من مقنه في شبكة البريد الإلكتروني ، وطاف هذا البرنامج بطول وعرض الولايات المتحدة ومثل عمل آلاف الكمبيوترات .. فقد كانت الدودة تتكاثر داخل الشبكة بطريقة استعصت على السيطرة ، وكانت تراجم ذاكرة الكمبيوتر المصاب وتقتله برا جزرا جزرا حتى ينزل وسط التخزين بالكامل .



والآلة ألا توجد طريقة نتقى بها شر الفيروسات  
والديدان؟ الحقيقة أنه المعركة طويلة والضربات  
قوية وفي كل يوم نسمع عجبا .. ولكننا نلقت الانظار  
لما يلي :

• أكرر الطرحه سهوله للانتقال الفيروس من كمبيوتر  
الى كمبيوتر هي "الديسكيتات" (Diskettes) .. لذلك  
يحظر دخول ديكيكات من الخارج الى حجرة الكمبيوتر ،  
ويراعى دائما أنه تستخدم ديكيكات جديدة واردة  
في أغلفتها الأصلية .

• تنتشر الفيروسات أيضا عن طريق تبادل برامج  
الألعاب الكمبيوترية (Computer games) .. فالمبرمج  
يُدس مجموعة تعليمات فيروسية في برنامج اللعبة  
و"يريد" بدونه مقابل لعدد من معارفه الذين  
يقومون بتحميله في ذواكر كمبيوتراتهم .. ومن هنا  
تبدأ العدوى في الانتقال الى البرامج السليمة التي  
تدخل لكل ذاكرة .

• يجب الحذر من البرامج التي تأتي لك بدونه توقع  
من شركات غير معروفة ولم يسبق لك التعامل معها .

• توجد برامج للكشف عن الفيروس  
(Virus-scanning software)  
وهذه يجب استدامها للتحقق من سلامة أى ملف



قبل تحميله على الأقراص الصلبة (Hard disks).

• إذا استعار واحد من أصدقائك ديسكيتات خاصة بك وأعادها إليك ، فيجب أن تتحقق من سلامتها بواسطة برامج الكشف عن الفيروس قبل أن تستخدمها مرة ثانية.

• توجد برامج لمحاربة الفيروس

(Antivirus software)

وهي برامج مصممة خصيصا لإيقاف انتشار الفيروس ومحاصرته ومحاولة القضاء عليه .. ويمكن استنساخ هذه البرامج أيضا للتحقق من سلامة القرص الصلب في كل مرة يبدأ فيها العمل على الكمبيوتر أو بصفة دورية بمجانية لك.

كلمة ٦-٢ أمان شبكات الكمبيوتر

(Computer network security)

تطرح شبكات الكمبيوتر مشكلات أمنية معقدة وذات طبيعة خاصة ، فالشبكة مترامية الأطراف ، ومجالات العمل عليها واسعة ومتعددة ، وعدد مستعمليها يفوق الحصر ، والاتصالات والارتباطات تتم مع عدد كبير في أجواء غامضة .  
فما هي مقومات سياسة الأمن تحت هذه الظروف ؟  
في البداية يوجب الاهتمام إلى نظم تشغيل الشبكة (Network operating systems) حيث تؤخذ اعتبارات



أمنية أساسية مثل ضرورة التحقق من شخصية المتقدم،  
عن طريق كلمات الرمثلا .

وفي معظم الشبكات توجد إمكانات التصريح للمستخدمين  
بالاستفادة من خدمات معينة بعه خدمات أخرى ، فقد  
يسمح لجميع العاملين بأحدى الشركات باستخدام برامج  
تنسيق الكلمات (Word processing) بينما يقصر  
الاطلاع على ملفات إنتاج وأرباح الشركة على عدد محدود  
من المسؤولين .. كما توجد إمكانات وضع حد أقصى لعدد  
مرات استخدام ملفات البيانات ، فيتم رصد أسماء  
الملفات وعدد المرات الفعلية التي تعامل فيها المتقدم  
مع كل ملف .

وتم التوصل إلى أسلوب فني لدعم أمن الشبكات  
يسمى "هائط النيران" (Firewall) .. وهائط النيران  
هذا كمبيوتر معين يتم تخصيصه - من بين كمبيوترات  
شبكة الشركة - للاتصال بمفرده بالعالم الخارجي  
(Outside world) ، بدلا من الاتصال الخارجية  
المفتوحة التي يمكنكم أنه تتم مع كمبيوترات الشبكة المتعددة  
ويصعب مراقبتها وإحكام السيطرة الأمنية عليها .

ومن برامج هائط النيران أيضا الاحتفاظ بقائمة أرقام  
تليفونات الجولات الخارجية التي توافقها الشركة لولا على  
التعامل مع شبكتها .. فتتصل الجبهة أولا بكمبيوتر هائط  
النيران وتطلب الوصول إلى الشبكة .. فإذا كان رقم تليفونه  
هذه الجبهة ضمن القائمة التي يحتفظ بها الكمبيوتر ، يعيد  
الكمبيوتر الاتصال بالجبهة وينبئها بأنه وصول لخط الشبكة



متاح ، ومنه هنا يبدأ الاتصال .. أما إذا لم يكن رقم  
تليفونه الجيزة الطالبة ضمن القائمة فلا يعيد الكمبيوتر  
الاتصال بها مانعا بذلك أى تعامل لها مع الشبكة .. لهذا  
أنه لا خوف من معرفة الجيزة الخارجية (غير المرغوب فيها)  
لرقم تليفونه هاتط النيران ، فتمام عمليات الاتصال  
بالشبكة مرهونه بمعرفة هاتط النيران لأرقام تليفونات  
الجيزات الخارجية .

وبالإضافة إلى فرصة الرقابة على الاتصالات التى تأتى  
للتبكة من الخارج ، ينبغي على الشركة أنه تولى اهتماما  
لشكلة التدخل غير المشروع فى البيانات وهى لازالت على  
الطريقه أثناء انتقالها من مكان إلى مكان .. فهناك لصوص  
وهواميس يأتون لارتكاب جرائمهم الكمبيوترية على  
طريقة قطاع الطرق .. ويمتلك توفير الحماية للبيانات  
فى هذه الحالة بواسطة عمليات "التشفير"  
(Encryption) .. فتكتب البيانات طبقا لشفرة  
خاصة لا يعرفها إلا المرسل عند بداية خط الاتصال  
على الشبكة ولا يقدر على فك رموزها إلا مستقبلها  
عند طرف الاتصال الآخر .. وقد تم تصميم شفرات  
قياسية لهذا الغرض منها "المواصفة القياسية لتشفير  
البيانات" [Data Encryption Standard (DES)]  
الاعتمدها المعهد القومى الأمريكى للمواصفات وتتم  
الآن على نطاق واسع .

وتوجد برامج تشفير (Encryption software) كذلك  
للكمبيوترات الشخصية حيث تستخدم لتشفير الملفات



وإغلاقه لوحات المفاتيح وحماية كلمات السر .

## ٧-٢ اعتبارات الخصوصية (Privacy)

في حياتنا اليومية نضطر لإعطاء بيانات ومعلومات  
تخصنا إلى العديد من الجهات والأفراد .. فما أكثر  
الاستمارات التي نملؤها لاستخراج البطاقات الشخصية  
أو العائلية ، تحرير عقود الزواج ، الالتحاق بعمل جديد ،  
الاشتراك في ناد رياضي ، تدبير الضرائب ، أداء  
الخدمة العسكرية ، دخول مستشفى للعلاج ، رفع دعوى  
قضائية ، المطالبة بمعاملة أو تأميم اجتماعي ، السفر  
للخارج ، شراء بضائع عبر طريق البريد ، المشاركة في  
عمليات التعداد وقياس الرأي العام ... الخ .  
وقد لا نتطيع هذه الطرق التي يتم بها جمع بيانات  
عنه المواطنين ، ولكننا نتطيع أنه نقول بكل تأكيد  
أيضا تذهب هذه البيانات : إلى ملفات الكمبيوتر .

## ١-٧-٢ تمرير بياناتك الشخصية من مكانه إلى آخر (Passing your personal data around)

إذا كنت قد أعطيت كل هذه البيانات ، فأين هي الآن ؟  
هل تم نقلها إلى جهة أخرى ؟ هل تم تأجيرها ؟ بيعها ؟  
من الذي اطلع عليها ؟ هل يمكنك الوصول إليها ثانية ؟  
أو بعبارة مختصرة أكثر صراحة ، هل بقي شيء خاص بك ؟



الحقيقة أنه - في عصر المعلومات المهيمنة وفطوط  
الاتصال فائقة السرعة - يسهل جدا نقل بياناتك من  
كمبيوتر الى كمبيوتر ومن شبكة الى شبكة .. ومن ثم  
تصبح - وربما تتحول - معرفة أماكن وجود بياناتك  
في أي وقت لا هو لإدلائك بها .

ويتم نقل البيانات الشخصية لأسباب كثيرة .. فمثلا  
في الولايات المتحدة ينقلونه بيانات الأفراد من سجلات  
"خدمة الإيرادات الداخلية للدولة"

[Internal Revenue Service (IRS)]

إلى سجلات الخدمة العسكرية لضبط المتخلفين عنه  
التجنيد ، وكذلك إلى سجلات قروض الطلاب لمعاقبة  
من لم يلتزم منهم بالداد .. ويثير تحرير البيانات من  
مكانه إلى آخر على هذا النحو جدلا واسعا على المستويين  
الرسمي والشعبي .

وفي بعض الأحيان ينبغي الرأي العام في منع تداول  
البيانات الشخصية .. حدث أنه أعلنت شركة خاصة  
عنه قرينة طرح أقراص مدمجة (CD - ROM) في  
الأسواق تحتوي على بيانات كاملة عنه كل مواطن أمريكي ،  
وأثار هذا الاعلان موجة عارمة من الاحتجاج والنفور  
اضطرت معها الشركة إلى إلغاء مشروعها .

ومع ذلك يسيطر القلق على الناس لاكتقادهم أنه  
أي بيانات يخصهم - مهما كانت درجة حساسيتها - سيجد  
طريقا عبر المسالك والبوابات الكمبيوترية إلى من  
يدفع الثمن .. وفي محاولة لإعارة الاحترام ورد



الاعتبار لخصوصية الانسان التي انتزعتها الكمبيوتر ،  
بدأت التشريعات القانونية تقول كالمعتاد .

### ٢-٧-٢ قوانين حماية الخصوصية (Privacy legislation)

لجأت معظم الدول الى وضع قوانين حماية الخصوصية  
لشاعة جو الطمأنينة بين مواطنيها .. ونشير الى القوانين  
التي الآتية المعمول بها في الولايات المتحدة :

#### (١) قانون تصحيح بيانات الذمة المالية (Fair Credit Reporting Act)

ظهر هذا القانون عام ١٩٧٠ وهو يعطي المواطن الحق  
في معرفة تفاصيل سجلات ذمته المالية والاعتراض عليها اذا  
لم تكن صحيحة .. فريضة السجلات يتم ايداعها في ملفات  
الكمبيوتر بعد استيفاء بنودها من مصادر متعددة بعيدة  
عنه ذه المواطن العادي ، وكأنه الناس يفاجأونه  
باتهامهم باعطاء بيانات مضللة عنه موافقهم المالية  
وهم لا يعرفونه - وليس لهم أنه يعرفوا - أسباب هذا  
الانحراف .. أما الآن فلا أي مواطن الحق في الاطلاع على  
ما تم جمعه عنه من معلومات تتعلق بوضعه المالي  
للتأكد بنفسه من صحته ودقتها ، وله أنه يصح ما قد  
يجده من بيانات مخالفة لحقيقة الوضع .



(٢) قانون حرية المعلومات

(Freedom of Information Act)

ظهر هذا القانون أيضا عام ١٩٧٠ وهو علامة بارزة في تشريعات حماية الخصوصية ، وينص على أنه للمواطن العادي الحق في الاطلاع على جميع المعلومات التي جمعتها عنه الهيئات الرسمية الفيدرالية ( وانه كانه الكشف عنه المعلومات يحتاج في بعض الأحيان الى حكم قضائي ) .

(٣) قانون الخصوصية الفيدرالي

(Federal Privacy Act)

ظهر هذا القانون عام ١٩٧٤ ويعتبر أكثر القوانين تأثيرا في مجال حماية خصوصية الأفراد ، إذ يرسى مبدأ قانونيا هاما : " يجب ألا تكون هناك أية ملفات سرية عن المواطنين " .. فكل مواطن مسجوع له بمعرفة ما يخصه من بيانات مخزونة في ملفات كمبيوترية أينما تكونه ، وله أنه يعرف الأغراض التي تستخدم فيها هذه البيانات ، كما أنه هو تصيحرا مكفول له على الدوام .

ويقضي القانون كذلك بأنه تعلم الهيئة التي تجمع بيانات شخصية عن المواطنين مبررات مقنعة للقيام بهذا العمل ، وأنه يكون المواطن على علم مسبوق بذلك .

(٤) قانون حماية خصوصية التسجيلات المرئية

(Video Privacy Protection Act)

ظهر هذا القانون عام ١٩٨٨ وهو يمنع تداول



التسجيلات المرئية (الفيديو) الخاصة بالاختصاص، إلا بعد موافقتهم.. ويطلب أنصار الخصوصية بتعميم ذلك على الملفات الطبية وملفات التأمين.

(٥) قانون المضاهاة بالكمبيوتر وحماية الخصوصية  
(Computer Matching and Privacy Protection Act)

ظهر هذا القانون عام ١٩٨٨ وهو يمنع الرئيات الحكومية من مقارنة ملفات الشخص المختلفة بقصد المضاهاة.. (ومع ذلك فعمليات المقارنة لازالت تجري بدونه تنظيم حقيقي).

٣-٧-٢ الخصوصية في مواقع العمل  
(Privacy in the workplace)

بالرغم من أنه العاملي لا يتوقعونه أنه يتمتعوا بخصومية كاملة وهم في مواقع عملهم، إلا أنهم عادة يعابونه بصدمة كبيرة عندما يكتشفونه أنهم واقعونه تحت مراقبة رئيسهم، وتعلوا أصواتهم: "لا بد من القضاء على هذا التجسس" .. والحقيقة أنه رئيس العمل لا يقصد أنه يتجسس على العاملي، ولكنه يدير مؤسسته بامكانيات الكمبيوتر المتقدمة.

وقد اهتمت النقابة القانونية حول هذه النقطة بظهور "برامج المراقبة" (surveillance software)



المهمة فصيقلًا لمراقبة أعمال الموظفين من كل مكان  
بالمؤسسة .. فبنفسطة بسيطة على مفتاح الفأرة  
(Mouse) يستطيع الرئيس أنه يرى أمامه ما هو  
ظاهر في أي وقت على شاشة أي موظف أثناء  
أداء عمله .

وليس الأمر قاصرا على رؤية مشاشات الموظفين  
عنه بعد ، ولكن برامج المراقبة قادرة أيضا على مراجعة  
رسائل البريد الإلكتروني لكل موظف ، ومعرفة عدد  
ضربات في الحقيقة على لوحة المفاتيح ، ورصد طول  
فترة استراحتهم ، وتحديد الملفات التي تعامل مع  
والمدرة التي استغرقها هذا التعامل .

وتتعدد اتصالات العمال ببرامج المراقبة ، وتقول بأنه  
العاملية الذي يقومون خرية "للجسس" يعانون  
من ضغط نفسي تفوق طاقة اهتمامهم .. ولكن  
شركات إنتاج برامج المراقبة تجزم بأنه هذه البرامج  
ليست للجسس ، وإنما هي اليد اليمنى للرئيس  
في إدارة أعماله بأسلوب عصري .

ويؤكد أنصار الخصوصية جهودهم في سبيل فرض  
ضوابط على عمليات المراقبة في مواقع العمل ، ويحاولون  
استصدار قانون يعطي العاملين الحق في تنبيه زميلهم  
عندما يسلط عليه رئيسه عيون المراقبة الكمبيوترية .

## ٨-٢ الاعتبارات الأخلاقية (Ethics)

في مجال العمل الكمبيوترى نرى ونسمع كل يوم



- كثيراً ما قصص المخالفات والتجاوزات الضارة بالعمل ولا تتكلم في الواقع إلا أخلاقيات الانسنة :
- فتشاهد شخصاً يتعامل مع الديكيات في مكان عمله باستهتار ورعونة ، وقد يترتب على ذلك تلف ديكيات زاهرة بملفات البيانات .. والبيانات - كما علمنا - هي المورد (Resource) الحيوى الذى يصعب جداً - وربما يستحيل - إصلاحه أو استبداله .
- وتسمع عنه موظف يتعمد البحث خلسة في ملف الأجور (Payroll file) ليعرف راتب زميل له لا يرغب في إطلاعه عليه .. وقد يصل التلصص على البيانات - مع شخص فاقد الضمير والقيم - إلى حد بيع أسرار عسكرية قومية إلى جهرات أجنبية ..
- وتقاها بأحد أصدقائك وقد واثته الجرأة لكن يضعك في موقف هرج ويطلب منك "استعارة" كلمة السر الخاصة بالعمل على كيبوترات معمل كطيقك .
- وتقدم في طالب زميلك نى معافى الأمانة والشرف ، ودبر فطة للاختراق هواجز أسم المنظومة الكمبيوترية فى الكلية واستطاع تغيير درجات امتحانات بعض المواد له ولأصدقائه المتواطئين معه .
- وربما تكونه اعتدت - بحكم المنافع المحيطة - على نسخ البرامج دونه أنه تكلف نفسك التفكير فيما إذا كان هذا النسخ مشروعاً أم غير مشروع .. والحقيقة أنه أخطر القضايا الأخلاقية الكمبيوترية هى تلك التى تتعلق بالنسخ غير القانونية (Illegal copies) التى



انتشرت - للأسف - على نطاق واسع في كل مكان ،  
وتعتبر مكالات متفاحمة تشبه بالشكوى منزا جميع  
الشركات الكبيرة والصغيرة على السواء .. وتفرد لرا  
هنا مناقشة مستقلة ..

### ١-٨-٢ نسخ البرامج (Copying software)

لم يعد مستغرباً أنه يتم تصوير جزء من كتاب أو الكتاب  
بأكمله على ماكينة تصوير مستندات وكذلك نسخ شرائط  
الأغاني وما شابهها على أجهزة التسجيل .. ورغم أنه  
العملية - تصوير الكتب ونسخ الأغاني - مخالفة  
للقانون ، إلا أنه يتكرر حدوثها كل يوم ونادراً ما يقع  
الفاعل تحت طائلة القانون .. وبأسلوب لا يختلف كثيراً  
يتم نسخ برامج الكمبيوتر على اختلاف أنواعها ، ولكنه  
المخالفة في هذه الحالة تنطوي على عواقب أخطر :  
فعملية تصوير كتاب تحتاج لجهود ووقت وصورة  
الكتاب لا تكون أبداً في نفس جودة الكتاب الأصلي ،  
أما نسخ برامج الكمبيوتر فعملية يسيرة وخطأ تخرج  
نسخة البرنامج مطابقة تماماً للأصل البرنامج وتؤدي  
وظيفته بنفس الدرجة من الكفاءة .. هذا بالإضافة  
إلى الاعتبار المادي الرام ، فنسخ شريط أكثر  
الأغاني نجاحاً ورواجاً لا يكلف الشركة المنتجة  
(والفنان) أكثر من عشرة جنيهات ، أما نسخ برنامج  
كمبيوتر فقد يكلف الشركة المنتجة (والمبرمج)



آلاف الجيولات .  
ويمكننا تقسيم البرامج هنا الى ثلاثة أنواع :

(١) البرامج المجانية (Freeware)  
وهي برامج يقوم بتصميمها متطوعوه أو هواه ويتم  
توزيعها مجاناً للجمهور .. وهذه البرامج مسموح بنسخها دون  
أية محاذير لأنه استخدام النسخ - بدلا من الأصول - لا  
يسبب ضارة للأحد .

(٢) برامج المشاركة (Shareware)  
وهي برامج يرسلها مصمموها الى المستخدميه مجاناً أيضاً ،  
ولكنهم - أي المصممين - يطعمونه في أنه يرسل لهم  
المستخدم - طواعية - مشاركة مادية كريمة إذا ثبتت له  
كفاءة البرنامج وفائدته .. ولا يوجد ما يمنع نسخ مثل هذه البرامج  
واستخدام النسخ بحرية تامة .

(٣) البرامج ذات حقوق التأليف والنشر (Copyrighted software)

هذه برامج قيمة متعددة الأغراض ويتكلف تصميمها كثيراً  
مثل برامج قواعد البيانات وتنسيق الكلمات والجداول الممتدة  
(Spreadsheets) .. وهي تباع بأسعار مرتفعة ،  
ويحظر نسخها إلا بموافقة الشركة المنتجة والتي تتمتع  
بحقوق التأليف والنشر .

ونسخ تلك البرامج بدون تصريح يعتبر سرقة ويطلع  
عليه أيضاً وصف "قرصنة البرامج" (Software piracy) ،  
لأنه النسخ يحرم الشركة المنتجة (ومصممي البرنامج) من  
الأرباح المشروعة المتوقعة .. لاحظ أنه ترك الجبل على



الفارب لقراصنة البرامج يجعل تصميم البرامج محلا غير مجز له يتصدى له ، وعليه يقل أو يتوقف إنتاج البرامج الجيدة الجديدة مما يعود بالضرر علينا جميعا — هل يستطيع كل واحد منا أن يصمم برامج تطبيقاته بنفسه ؟! ومع ذلك ننوء الى أنه ليست كل عملية نسخ برنامج برعة سرقة وليس كل ناسخ قرصانا .. فبعد أنه تشتري برنامجا ببضع مئات من الجنيئات ، سيته تفكيرك هتالما يلى :

- عمل نسخة بديلة للبرنامج لتغيرها عند الطوارئ.
- نسخ البرنامج على القرص الصلب لاستخدامه بمرونة أكثر.
- الاحتفاظ بنسخة من البرنامج فى مكانه محلك ونسخة أخرى فى منزلك.

ومعظم المنتجيه لا يلقوه بالا لعمليات النسخ التى من هذا القبيل .. ولكن هناك آلافا من مستخدمى الكمبيوتر يحترفونه النسخ لسبب آخر ومختلف تماما : الحصول على البرامج بدونه دفع ثمنها .. وهنا تكمن المشكلة .

## ٢-٨-٢ محاربة نسخ البرامج

(Fighting software copying)

كرمت شركات إنتاج البرامج جهودها للتغلب على مشكلة نسخ البرامج ، ونشيرها الى ثلاثة حلول مختلفة :

(١) وسائل منع النسخ (Copy protection)

لجأت الشركات فى البداية الى "وسائل منع النسخ"



التي تجعل البرامج تخرج من الشركة وهي غير قابلة للنسخ ..  
ولكنه قبل هذا الحل بمعارضة قوية من ستندى الكمبيوتر  
على أساس أنه منع النسخ نهائياً عقاب للمخزيين والأبرار  
أيضاً أو - بعبارة أخرى - مضايقة جموع الشرفاء من أهل  
مطاردة هفنة من اللصوص .. وتمت الضغط الجماهيري  
أقلمت الشركات مع هذا الاجراء .

### (٢) تصريح الموقع (Site licensing)

تلتزم بعض الشركات أسلوب "تصريح الموقع" والذي  
يعني عقد اتفاق مع العميل (موقع محل) بموجبه يصريح  
له بنسخ برنامج (استراة من الشركة) أي عدد من المرات  
يشاء، واستخدام جميع العاملين للنسخ بحرية كاملة  
في مختلف مراحل العمل .. ويكون التصريح مقابل مبلغ  
إضافي من المال يوافق عليه الطرفان.

### (٣) التصريح الآني (Concurrent licensing)

تتبع شركات أخرى - في مقدمتها شركة "ميكروسوفت"  
(Microsoft) الشهيرة - إلى أسلوب "التصريح الآني"  
وهو نظام يقرر المقابل المالي لتصريح نسخ البرامج على  
أساس عدد المستخدمين للبرنامج في آن واحد (ساعة  
ذروة العمل مثلاً) .. حسب أنه ٣٠ موظفا يعملونه على  
شبكة كمبيوترية بأحدى المؤسسات، ولكنه ١٠ منهم  
فقط هم الذين يستخدمونه برنامج "ميكروسوفت إكسل"  
(Microsoft Excel) في نفس الوقت في مرحلة  
عمل معينة .. عندئذ تدفع المؤسسة ثمنه ١٠ نسخ  
من البرنامج للشركة المضيفة.